Fraud Presentation

State of North Dakota

J.P.Morgan

What is Fraud

Fraud

- Fraud involves the unauthorized use of a Card—whether by the cardholder, other internal employees and/or outside parties, resulting in one or more acquisitions whereby the end-user organization does not benefit.
- This includes crimes such as a cardholder's use of the card for personal gain, use of stolen cards, account numbers and counterfeit cards.

Misuse

- Misuse involves unauthorized activity by the employee to whom the card is issued.
- The employee has misused the card by not being compliant with internal policies and procedures for personal gain.

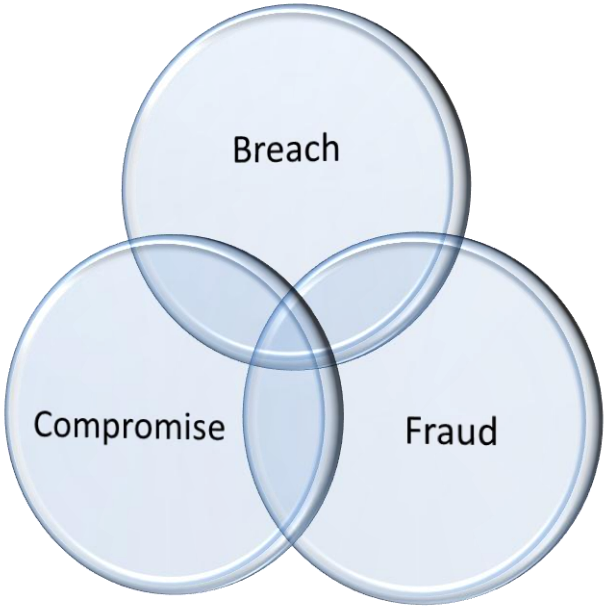
Methods of Obtaining Fraud Information

Breach: Data Compromise at the Merchant or a Merchant Processor

Compromise: Account data is in the possession of people with malicious intent

Fraud: Confirmed non-authorized use of an account

Magnetic Stripe Data:
Card Number
Name
Expiration Date
PIN Verification Data: defines and decrypts PIN
Card Verification Value – CVV: unique identifier to specific card



Current Industry Trends

- Gift Cards- counterfeit card used to purchase gift cards from a retail merchant
- Day to Day Living Expenses- not as easily detected in the tools
- Gas Pumps- most common in states with fewer controls
- Counterfeit Fraud- one of the fastest growing forms of fraud
- Test Merchants- method in which fraudsters test the status of the card

Probing

Definition: A merchant is fraudulently used (without their knowledge) to test the validity of an account number

Types of probing

- Taking over merchant ID / dummy terminal
- Hacking into merchant's system
- Fraudulently opening a new merchant / business
- Computer algorithm
- Simple swipe at gas pump (less common)

What is Skimming?

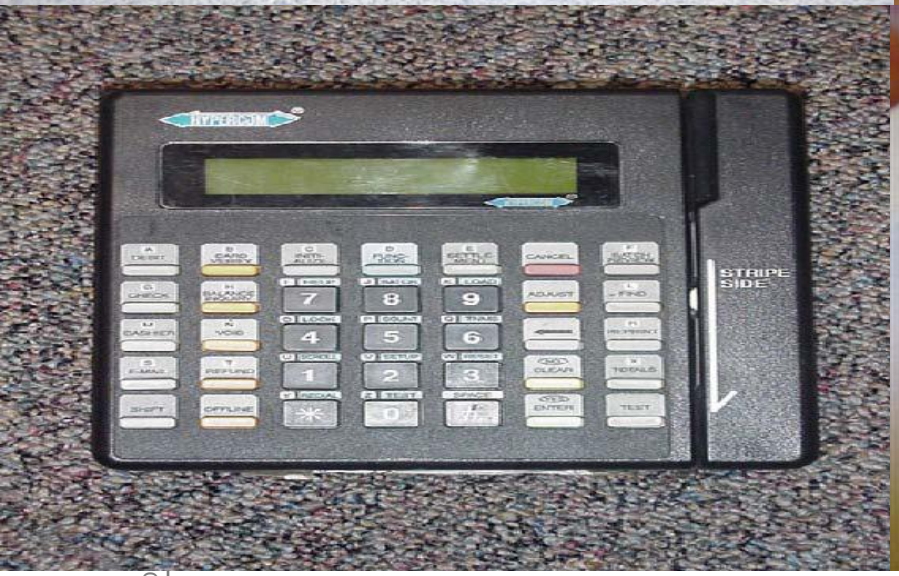
The copying of electronically transmitted full track data on the magnetic strip of a credit card, to enable valid electronic payment authorization to occur between a merchant and the issuing financial institution.

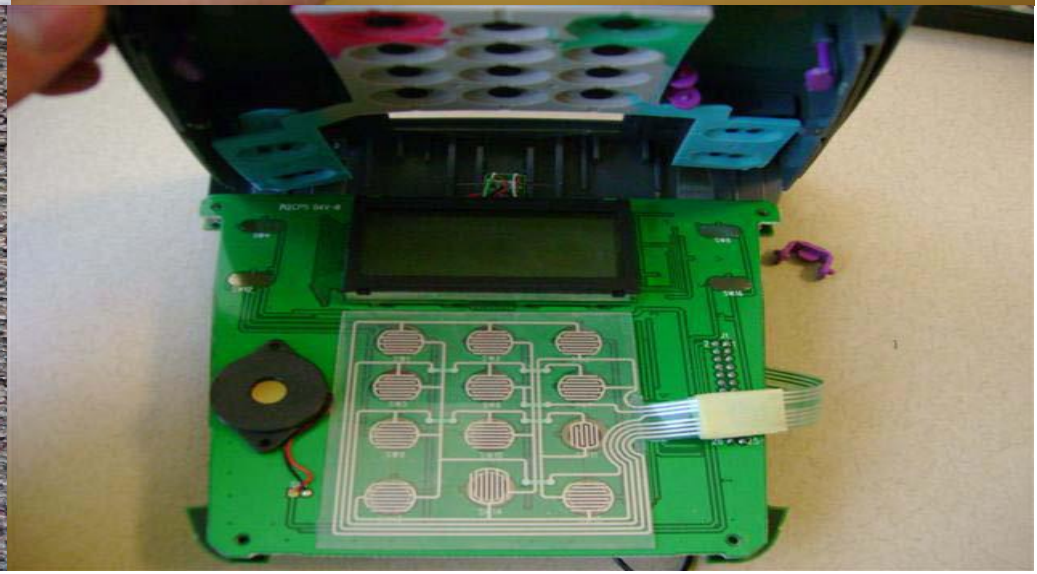
The stolen data / information is re-encoded on "white plastic" or counterfeit cards to make unauthorized withdrawls.

Why is skimming so popular

- The equipment is available over the internet
- The software and hardware are very user friendly and extremely mobile
- The skimmed information can be transmitted via email anywhere in the world within hours after it is skimmed.
- Cardholders are not aware that they have been victimized until they see the statements.

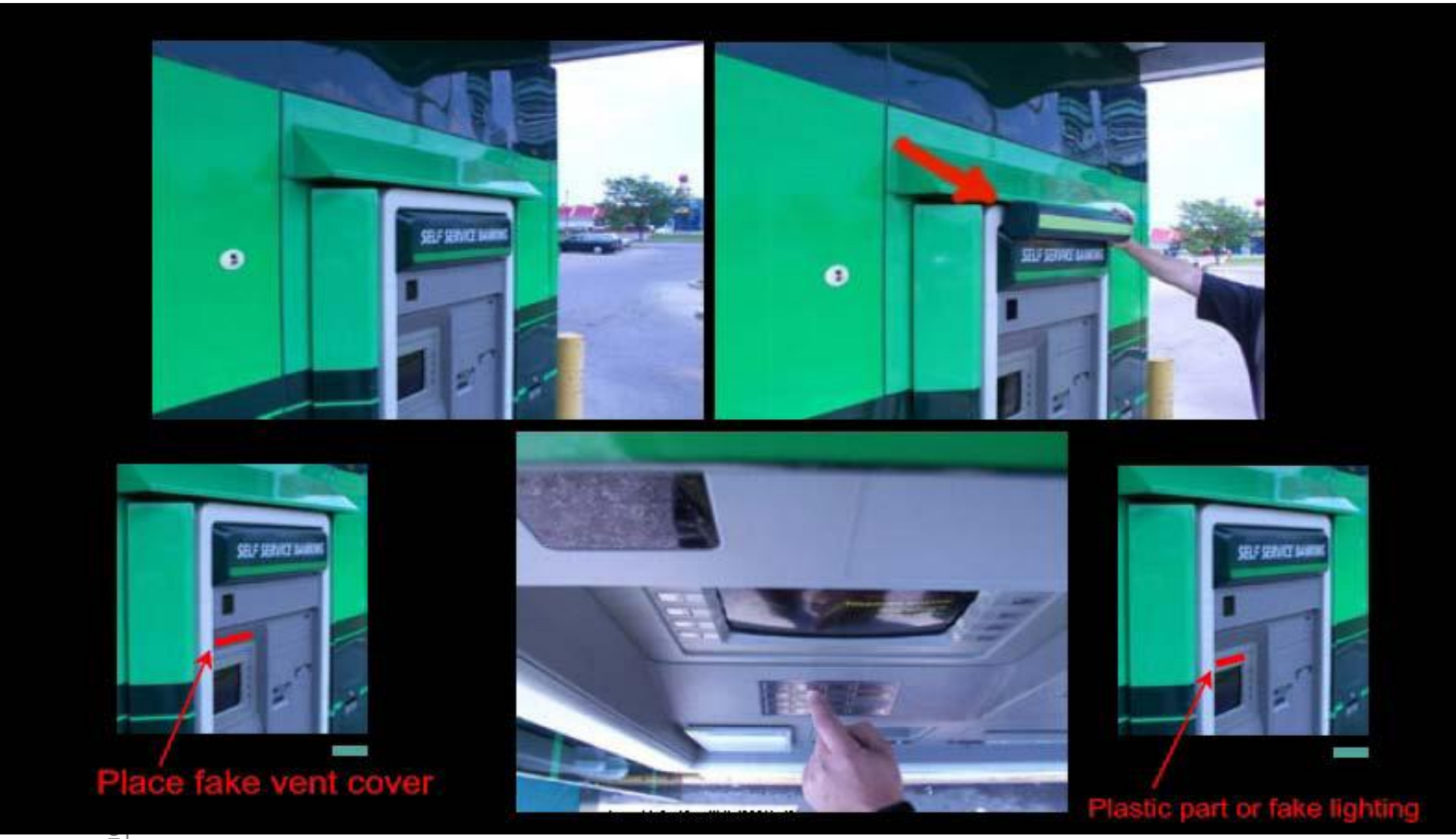
Skimming Devices



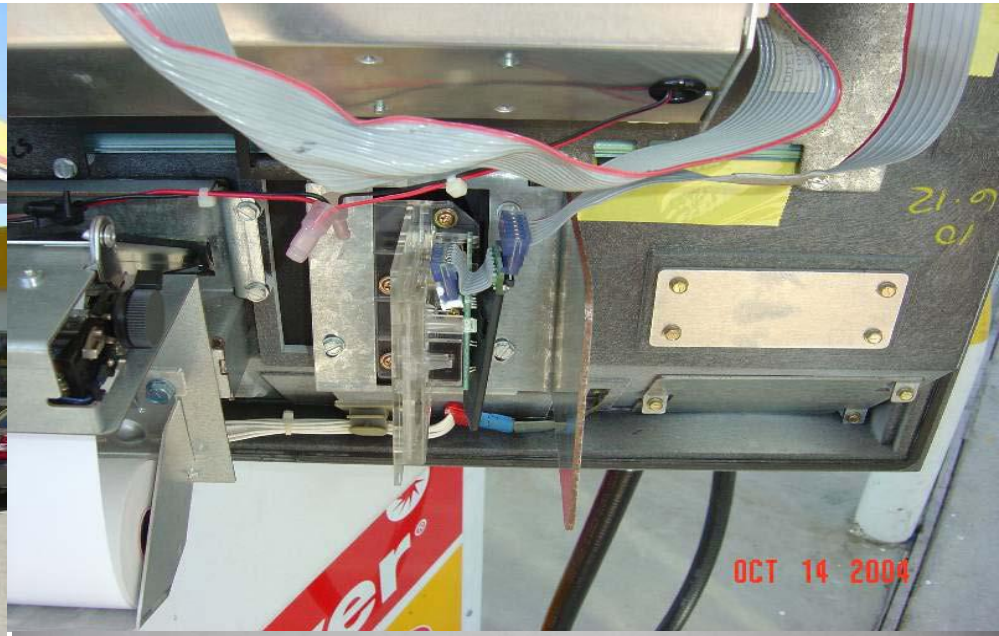


Skimming Devices

Skimming Devices



Skimming Devices – Gas Pumps



Account Compromise

Definition: Visa and MasterCard alert JP Morgan to accounts that have been confirmed compromised

Types of compromise

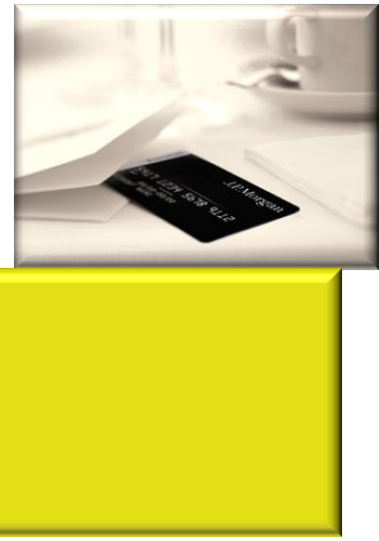
- Hacking event
- Dishonest employee
- Theft of documents

Compromise example

- $32.00 at American Airlines is last valid trans(2/12/2010 at 15:35)
- Account closed due to notification of compromise from associations (2/12/2010)
- Three fraud casino cash transactions attempted (3/13/2010 through 3/14/2010)

Client Best Practices

- Utilize the card controls available
  - Implement velocity limits on MCCs
  - Review and set credit limits based on usage
  - Limit cash access
- Review transaction reports for exceptions and declines
- Educate your cardholders to:
  - Review their transactions and statements
  - Utilize bank owned facilities and ATMs when getting cash
- Use account blocking for temporary leaves or infrequent travelers
- Notification of Voluntary/Involuntary Terminations



Employee Awareness

- Internal Policies
  - Communicate Internal Policies upon Program Administrator approval of Company Credit Card
  - Immediately Report a Lost/Stolen card to JPMorgan
  - Keep JPMorgan's Customer Service telephone number separate from the card in case it is lost or stolen
  - Highlight consequences of misuse
    - Termination of Employment
  - Internal Audit
    - Scorecard
      - Review "x" number of accounts
      - Questionable activity based on company usage

Employee Awareness Scripting

- When receiving a phone call from a JPMorgan Commercial Card Representative, it is not JPMorgan practice to ask you to provide:
  - Your complete social security number, a representative may ask for the last 4 digits as a verification point
  - Card's expiration date
  - CVV or CVV2 from the back of your card
- A Commercial Card Representative may ask you for your account number (usually when returning a message you have left) and it is our practice to verify at least one piece of personal information.
- If you are in doubt, do not provide any personal information to the caller and call the 800 number listed on the back of your card to report the incident.

Employee Awareness Phishing

- Phishing is an attempt to gain private information about you and your accounts. Most often via e-mail that looks like it is from your financial institution.
- It is not JPMorgan practice to:
  - Send e-mail that requires you to enter personal information directly into the e-mail
  - Send e-mail threatening to close your account if you do not taken immediate action of providing personal information
  - Send e-mail asking you to reply by sending personal information
  - Send e-mail asking you to enter your user ID, password, or account number into an e-mail or non-secure web page

You should never reply to click on or enter any information if you receive a suspicious e-mail.

If you are unsure if the e-mail is legitimate call the 800 number on the back of your card